REMARKS

With the foregoing amendment claims 1-7 and 14-20 and 25-44 are pending in the application. Claims 1-3 are independent. No new matter has been added by the amendments. Applicant respectfully requests reconsideration of the Rejections/Objections, which are discussed below.

Objection to Claims for Lack of Antecedent Basis

Claims 4, 17, 25 and 26 have been objected to for lack of antecedent basis. Claims 4, 17, 25 and 26 have been amended to clarify their antecedent basis.

Rejection of Claims 1 and 2 under 35 U.S.C. § 103(a)

Claims 1, 2, 8-13 and 21-24 were rejected as obvious over U.S. Pat. 7,152,242 to Douglas and in view of U.S. Pat. 6,640,242 to O'Neal. Applicant respectfully disagrees.

Independent Claim 1

With respect to independent claim 1, claim 1 is patentable over the art because the art, considered alone or in combination, does not teach or suggest all of the feature of claim 1, as currently amended. Claim 1 has been amended to include the feature of claim 10 as was previously presented. More specifically, claim 1 now requires "a deterministic network" and requires that both the challenge and the response be transmitted via the deterministic network. Neither Douglas nor O'Neal teach or suggest this feature.

With respect to Douglas, Applicant agrees with the Office's conclusion that Douglas does not disclose a challenge handler configured to receive a challenge from an external monitor and provide a response thereto. And, thus, does not disclose sending a challenge or response via a deterministic network.

With respect to O'Neal, Applicant admits that O'Neal discloses a "network" and a monitor that periodically transmits messages to the systems that it is monitoring. However, claim 1 explicitly requires a "deterministic network." O'Neal does not disclose a deterministic network. Rather, O'Neal discloses a monitor 216 that "periodically sends a message to each of systems 2008-2016 and each of a number of sub-systems eliciting response messages from each." Col. 19, lines 11-25. It is clear from FIG. 20 of O'Neal that the monitor 216 sends the message to the systems 2008-2016 using local area network (LAN) 2022. O'Neal does not teach or suggest that LAN 2022 is a "deterministic network." Furthermore, the Office in its rejection of claim 10 as previously presented, did not even allege that O'Neal discloses a "deterministic network." Rather, the Office merely alleged that O'Neal discloses a network. The reason the Office can not even allege that O'Neal discloses a deterministic network is because such a network is simply not disclosed in O'Neal.

Accordingly, because neither of the references cited by the Office teach or suggest a deterministic network, the rejection of claim 1 should be withdrawn.

Claim 1 also requires that "the external monitor is configured so that if the external monitor does not receive the response within five milliseconds or less from sending the challenge, the external monitor issues a notification and/or shuts down at least part of the computer system or application." This feature is not taught or suggested by O'Neal.

Applicant admits that O'Neal discloses a monitor that is configured such that if the monitor does not receive a response within a predetermined amount of time from sending a challenge, the monitor issues a notification. However, nowhere does O'Neal teach or suggest that the predetermined amount of time could be as little as 5 milliseconds.

The reason that O'Neal does not teach or suggest that the predetermined amount of time could be as little as 5 milliseconds is because the system disclosed in O'Neal would not function properly if the predetermined amount of time was so small. The reason the system would not function properly is because, even if each system being monitored by the monitor 216 was fully functional and able to quickly respond to the message transmitted from the monitor 216, the monitor 216 may not receive the response within 5 milliseconds due to the fact that the response must travel through LAN 2022 and, if the traffic on the LAN was heavy (which is likely), the response would be delayed. In other words, if the "predetermined amount of time" was set to 5 milliseconds or less, the monitor 216 would undoubtedly generate several false alarms due to the simple fact that the traffic on the LAN 2022 is heavy, thereby delaying the monitor from receiving the response. Accordingly, O'Neal does not teach or suggest "5 millisecond or less" feature of claim 1. For this additional, independent reason, the rejection of claim 1 should be withdrawn.

Finally, claim 1 also requires "a real-time operating system." The Office contends that Douglas discloses a "real-time operating system." Applicant respectfully disagrees.

Applicant admits that Douglas discloses a "host-based intrusion detection system (HIDS) sensor ... running in real time ...." *See Abstract.* The term "real time" has several distinct meanings in the field. In this case, Douglass clearly means "continuous", while applicant mean "respecting timing deadlines." Thus, Douglass' discloses a system that detects intrusions "continuously" and Applicant discloses a system that relies on deadlines to detect intrusions. These are not similar.

Furthermore, the HIDS sensor disclosed in Douglas is an application that runs on an operating system, it is not an operating system itself. Moreover, just because the HIDS sensor, which is an application, runs in real-time does necessarily mean that it runs on top of real-time operating system. In fact, Douglas explicitly discloses that the HIDS sensor is an application that runs on top of the Unix, Linux or Windows operating systems, none of which is a real-time operating system. Accordingly, even though Douglas discloses that the HIDS sensor application runs in real-time, Douglas does not disclose "a real-time operating system," which is required by claim 1. For this additional, independent reason, the rejection of claim 1 should be withdrawn.

Independent Claim 2

Similarly to claim 1, claim 2 requires: (1) "a real-time operating system," (2) "a deterministic network," and (3) "sending to the external monitor via the deterministic network a response to the challenge, wherein the response is sent in less than about five milliseconds from when the challenge was received." Accordingly, the above remarks for claim 1 apply to claim 2.

Rejection of Claims 3, 27 and 31 under 35 U.S.C. § 103(a)

Claims 3, 27 and 31 were rejected as obvious over REDSonic, Inc., "http://www.redsonic.com/en/products/RealTime.htm"; Copyright 2002, pp1-4, ("Sonic") and further in view of Douglas.

With respect to claim 3, from which claims 27-38 depend, this claim recites a second real-time thread being configured to monitor integrity of the first real-time thread. Applicant acknowledges that Sonic fails to disclose or suggest this feature. Douglas fails to cure this deficiency. Douglas teaches a host-based IDS sensor that monitors files. Douglas, col. 2, ll. 45-50. Monitoring a file does not disclose or suggest monitoring the integrity of a real-time thread.

Additionally, claim 3 requires "a security process running under the non-real-time kernel, the security process being configured to check the integrity of the first real-time thread and/or the second real-time thread." Applicant agrees with the Office's conclusion that Sonic fails to disclose or suggest this feature. Douglas fails to cure this deficiency. In fact, the Office does not even allege that Douglas discloses this feature. Rather, the Office simply notes that Douglas discloses a "HIDS sensor 20 [that] is capable of monitoring the integrity of the Linux kernel." Even if we assume for the sake of argument that the Linux kernel is a thread running under a real-time kernel, Douglas would still not disclose the feature in question because the Linux kernel does not (a) monitor the integrity of an application running under the non-real-time kernel or (b) monitor integrity of a thread that is configured to monitor the integrity of an application running under the non-real-time kernel. That is, neither the claimed "first thread" or claimed "second thread" reads on the Linux kernel disclosed in Douglas.

Lastly, because Douglas does not disclose a dual-kernel operating system that includes a real-time kernel and a non-real-time kernel, it is impossible, by definition, for Douglas to disclose a first and second thread running under the real-time kernel and a process running under the non-real-time kernel. Accordingly, Douglas can simply not make up for the deficient teachings of Sonic.

For each of the above reasons, Applicant respectfully requests that the rejection of claim 3 be withdrawn.

Rejection of Claims 4-5 and 17-18 under 35 U.S.C. § 103(a)

Claims 4-5 and 17-18 were rejected as obvious over Douglas and further in view of O'Neal and Williams et al. (U.S. Patent No. 5,911,065).

Claim 4

With respect to claim 4, from which claim 5 depends, this claim has been amended to recite wherein the integrity check performed by the security process includes checking an execution schedule of the application. With respect to Douglas and O'Neal, Applicant agrees with the Office's conclusion that neither Douglas nor O'Neal disclose this feature. Williams fails to cure this deficiency. Williams does not disclose a security process, let alone an integrity check performed by the security process that includes checking an execution schedule of the application. Williams merely discloses a task scheduling environment. There is simply nothing in Williams that teaches or suggests checking the integrity of an application by checking an execution schedule of the application. Accordingly, Williams can simply not make up for the deficient teachings of Douglas and O'Neal.

For each of the above reasons, Applicant respectfully requests that the rejection of claims 4 and 5 be withdrawn.

Claim 17

Similarly to claim 4, claim 17, from which claim 18 depends, recites wherein the integrity check performed by the security process includes checking an execution schedule of the application. Accordingly, the above remarks for claim 4 also apply to claim 17.

Rejection of Claims 6-7 and 19-20 under 35 U.S.C. § 103(a)

Claims 6-7 and 19-20 were rejected as obvious over Douglas and further in view of O'Neal and Terry. In rejecting claim 6, the Office contends that Terry discloses a system that checks the integrity of application code. In support of its contention, the Office cites to paragraph [0074] of Terry, which is reproduced below for the convenience of the Examiner.

> [0074] If the function in block 216, which determines if a registry modification has been made, identifies a modification, then the function reports (alerts) the administrative application 115 by generating and transmitting a structured signal file (block 218). If there has been no registry modification, then polling continues (217) for the defined registry segments by returning to the function in block 215.

It is clear that the above portion of Terry does not disclose checking the integrity of application code. Rather, it is clear that the above portion of Terry merely discloses a system that checks whether or not a "registry" (i.e., database) has been modified." The step of checking whether or not there has been a "registry modification" in no way teaches or suggests checking the integrity of application code.

Applicant wishes to emphasize that Applicant is not attempting to cover every security system that performs any type of integrity check, but rather is attempting to cover only those systems that that are configured specifically as claimed, thus the existence of systems that check whether a database has been modified are not relevant to the claimed invention.

Rejection of Claims 25 and 26 under 35 U.S.C. § 103(a)

Claims 25 and 26 were rejected as obvious over Douglas and further in view of O'Neal and Berg et al. (U.S. Patent Pub. No. US 2001/0044904). Claim 25, from which claim 26 depends, recites sending an encryption key to the security process at or about the same time as sending the challenge to the security process. With respect to Douglas and O'Neal, Applicant agrees with the Office's conclusion that neither Douglas nor O'Neal . Berg fails to cure this deficiency.

Berg does not disclose a challenge. Accordingly, because Berg does not disclose a challenge, by definition Berg does not disclose sending an encryption key to the security process at or about the same time as sending a challenge to the security process. Berg merely discloses a system in which "the ... channel is authenticated and hardened." *Berg*, [0072]. There is simply nothing in Berg that teaches or suggests sending an encryption key to the security process at or about the same time as sending the challenge to the security process. Thus, Berg does not cure the deficiency.

Moreover, there is no reason to combine Berg with O'Neal. Berg discloses an encrypted communications channel. O'Neal discloses a message system and a monitor to determine whether or not the message system is operating properly. In particular, the monitor of O'Neal periodically sends a message to each of the systems eliciting a response from each. Col. 19, lines 11-16. The system of O'Neal only detects a failure if a system fails to respond. Col. 19, lines 16-18. Accordingly, if an attacker were to monitor the system of O'Neal, all that the attacker would need to determine is whether or not a response was elicited, not the content of the response. If an attacker were to detect an encrypted response, the attacker would still be able to determine that a response was sent. Conversely, if no response was elicited, encryption would not prevent the attacker from learning that no response was sent. Accordingly, there is no reason to encrypt the communications between the monitor and the system being monitored because the content does not contain any confidential information. Therefore, there is no reason to combine Berg with O'Neal, and thus Berg cannot make up for any deficient teachings of O'Neal.

For each of the above reasons, Applicant respectfully requests that the rejection of claims 25 and 26 be withdrawn.

Rejection of Claims 15 and 16 under 35 U.S.C. § 103(a)

Claims 15 and 16 were rejected as obvious over Douglas and further in view of O'Neal, Terry and Berg. Claim 15, from which claim 16 depends, recites wherein the security process is further configured to transmit the data item to the external monitor using an encryption key included in a challenge sent to the challenge handler. With respect to Douglas, O'Neal and Terry, Applicant agrees with the Office's conclusion neither Douglas, O'Neal nor Terry disclose this feature. Berg does not cure these deficiencies.

Berg does not disclose a challenge, let alone sending an encryption key to the security process at or about the same time as sending the challenge to the security process. Berg merely discloses a system in which "the … channel is authenticated and hardened." *Berg*, [0072]. There is simply nothing in Berg that teaches or suggests sending an encryption key to the security process at or about the same time as sending the challenge to the security process.

Moreover, there is no reason to combine Berg with O'Neal. Berg discloses an encrypted communications channel. O'Neal discloses a message system and a monitor to determine whether or not the message system is operating properly. In particular, the monitor of O'Neal periodically sends a message to each of the systems eliciting a response from each. Col. 19, lines 11-16. The system of O'Neal only detects a failure if a system fails to respond. Col. 19, lines 16-18. Accordingly, if an attacker were to monitor the system of O'Neal, all that the attacker would need to determine is whether or not a response was elicited, not the content of the response. If an attacker were to detect an encrypted response, the attacker would still be able to determine that a response was sent. Conversely, if no response was elicited, encryption would not prevent the attacker from learning that no response was sent. Accordingly, there is no reason to encrypt the communications between the monitor and the system being monitored because the content does not contain any confidential information. Therefore, there is no reason to combine Berg with O'Neal, and thus Berg cannot make up for any deficient teachings of O'Neal.

For each of the above reasons, Applicant respectfully requests that the rejection of claims 15 and 16 be withdrawn.

Rejection of Claim 36 under 35 U.S.C. § 103(a)

Claim 36 was rejected as obvious over Sonic and further in view of Douglas, O'Neal and Berg. Claim 36 recites_wherein the response includes an encrypted data item. With respect to Sonic, Douglas and O'Neal, Applicant agrees with the Office's conclusion neither Sonic, Douglas nor O'Neal disclose this feature. Berg does not cure these deficiencies.

Berg does not disclose a response, let alone that the response includes an encrypted data item. Berg merely discloses a system in which "the ... channel is authenticated and hardened." *Berg*, [0072]. There is simply nothing in Berg that teaches or suggests that the response includes an encrypted data item.

Moreover, there is no reason to combine Berg with O'Neal. Berg discloses an encrypted communications channel. O'Neal discloses a message system and a monitor to determine whether or not the message system is operating properly. In particular, the monitor of O'Neal periodically sends a message to each of the systems eliciting a response from each. Col. 19, lines 11-16. The system of O'Neal only detects a failure if a system fails to respond. Col. 19, lines 16-18. Accordingly, if an attacker were to monitor the system of O'Neal, all that the attacker would need to determine is whether or not a response was elicited, not the content of the response. If an attacker were to detect an encrypted response, the attacker would still be able to determine that a response was sent. Conversely, if no response was elicited, encryption would not prevent the attacker from learning that no response was sent. Accordingly, there is no reason to encrypt the communications between the monitor and the system being monitored because the content does not contain any confidential information. Therefore, there is no reason to combine Berg with O'Neal, and thus Berg cannot make up for any deficient teachings of O'Neal.

For each of the above reasons, Applicant respectfully requests that the rejection of claim 36 be withdrawn.

New Claims

New claims 39-44 are added. Claims 39-41 depend from claim 1. Thus, these claims are patentable for at least the same reasons give above with respect to claim 1. Claims 42-44 depend from claim 2. Thus, these claims are patentable for at least the same reasons give above with respect to claim 2.

Conclusion

All of the stated grounds of objection and rejection have been properly traversed, accommodated, or rendered moot. Applicant therefore respectfully requests that the Examiner reconsider all presently outstanding objections and rejections, and that they be withdrawn. Applicant believes that a full and complete reply has been made to the outstanding Office Action and, as such, the present application is in condition for allowance.

If the Examiner believes, for any reason, that personal communication will expedite prosecution of this application, the Examiner is invited to telephone the undersigned at the number provided.

In the event that this paper is not timely filed, the Applicants respectfully petition for an appropriate extension of time. Any fees for such an extension together with any additional fees may be charged to Counsel's Deposit Account No. 02-2135.

Respectfully submitted,

By ______________________

Brian Rosenbloom
Registration No. 41,276
Martin M. Zoltick
Registration No. 35,745
Attorneys for Applicant
ROTHWELL, FIGG, ERNST & MANBECK
1425 K. Street, Suite 800
Washington, D.C. 20005
Telephone: (202) 783-6040

#1430380